

"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Zastosowania kryptografii w Internecie				Implementation of Cryptography in Internet					
Kod przedmiotu	WCYKSCSI_ZKI.....ZKI									
Język wykładowy	polski									
Profil studiów	ogólnoakademicki									
Forma studiów	studia stacjonarne									
Poziom studiów	studia pierwszego stopnia									
Rodzaj przedmiotu	obowiązkowy									
Obowiązuje od naboru	2021/2022									
Forma zajęć, liczba godzin/rygor, razem godz., pkt ECTS	semestr	(x egzamin, + zaliczenie, # projekt)						punkty ECTS		
		razem	wykłady	ćwiczenia	laboratoria	projekt	seminarium			
	V	44+	20		24+			3.0		
	razem		20		24			3.0		
Przedmioty wprowadzające	● Matematyka dyskretna I - K_U03, K_U17, K_W02 ● Matematyka dyskretna II - K_U03, K_U17, K_W02									
Semestr/kierunek studiów	semestr 5 / Kryptologia i cyberbezpieczeństwo / wszystkie specjalności									
Autor	dr inż. Piotr Bora									
Jednostka odpowiedzialna za przedmiot	Instytut Matematyki i Kryptologii									
Skrócony opis przedmiotu	● Wykład, ćwiczenia laboratoryjne									
Pełny opis przedmiotu (treści programowe)	lp.	Semestr V temat/tematyka zajęć				liczba godzin				
						wkł.	ćw.	lab.	prj.	sem.
	1	Podstawowe usługi kryptograficzne: poufność, integralność, niezaprzeczalność, podpis cyfrowy, kryptowaluty				6		4		
	2	Pakiety ochrony poczty elektronicznej: PGP, PEM				2		8		
	3	System uwiarygodniania i autoryzacji: KERBEROS				4		4		
	4	Systemy wiązania bloków				8		8		
	Razem				20		24			
Literatura	podstawowa: ● Schneier B.: Kryptografia dla praktyków, wyd. II 2002 ● Stokłosa J., Bilski T., Pawłowski T.: Bezpieczeństwo danych w systemach kryptograficznych. 2001 uzupełniająca: ● Robling - Denning D. E.: Kryptografia i ochrona danych 1982									
Efekty uczenia się	Symbol	Efekty kształcenia						odniesienie do efektów kształcenia dla kierunku		
	U1	Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie								
	U2	Ma umiejętność samokształcenia się								
	U3	Potrafi - zgodnie z zadaną specyfikacją - zaprojektować i zrealizować prosty system lub proces komunikacji sieciowej w wybranych językach oraz technologiach, używając właściwych metod, technik i narzędzi, potrafi Posługiwać się nowoczesnymi środowiskami programowymi pozwalającymi na budowę i uruchomienie aplikacji internetowej pracującej w wybranym środowisku systemowym								
	W1	ma podstawową wiedzę z zakresu ochrony i bezpieczeństwa w systemach teleinformatycznych oraz szczegółową wiedzę z wybranych zagadnień z zakresu Marządzania bezpieczeństwem teleinformatycznym, w tym również budowy i wdrażania SZBI, akredytacji i certyfikacji urządzeń i systemów teleinformatycznych								
	W2	Ma uporządkowaną, podbudowaną teoretycznie ogólną wiedzę w zakresie zasad funkcjonowania sieci komputerowych i użytkowania podstawowych usług sieciowych oraz szczegółową wiedzę z zakresu projektowania i zarządzania sieciami komputerowymi w tym administrowanie sieciowymi systemami operacyjnymi								
	W3	Ma uporządkowaną, podbudowaną teoretycznie, szczegółową								

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku	
		wiedzę w zakresie projektowania i wytwarzania oprogramowania dla zastosowań sieciowych		
	W4	Ma ogólną wiedzę dotyczącą metod i technik kryptograficznych oraz ma uporządkowaną, podbudowaną teoretycznie, szczegółową wiedzę w zakresie matematycznych podstaw kryptologii, protokołów i systemów kryptograficznych oraz systemów zabezpieczeń	K_W23	
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	● Zaliczenie ćwiczeń			
Bilans ECTS (nakład pracy studenta)	SEMESTR 5			
	Aktywność	Obciążenie studenta		
		Liczba godzin	Liczba ECTS	
	Udział w wykładach	20	0.5	
	Udział w laboratoriach	24	1	
	Udział w ćwiczeniach	0	0	
	Udział w projektach	0	0	
	Udział w seminariach	0	0	
	Samodzielne studiowanie tematyki wykładów	10	0.25	
	Samodzielne przygotowanie do laboratoriów	20	1.25	
	Samodzielne przygotowanie do ćwiczeń			
	Samodzielna realizacja projektu	30		
	Samodzielne przygotowanie do seminariów			
	Udział w konsultacjach			
	Przygotowanie do egzaminu			
	Przygotowanie do zaliczenia			
	Udział w egzaminie / kolokwium			
	Sumaryczne obciążenie pracą studenta	104	3	
	Zajęcia z udziałem nauczycieli	44	1.5	
	Zajęcia powiązane z działalnością naukową	104	3	
	Zajęcia o charakterze praktycznym	74	2.25	

autor

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

dr inż. Piotr Bora

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr hab. Kojdecki Marek

tytuł, stopień naukowy, imię, NAZWISKO, podpis